Cloud Computing Security: Issues And Challenges

Tanvi Agrawal[1], Dr. Ambuj Kumar Agarwal[2], Prof. Dr. S.K. Singh[3]

[1]*Research Scholar, AIIT, Amity University, Lucknow*

[2]*Associate Professor, College of Computing Sciences and Information Technology*
Teerthanker Mahaveer University, Moradabad India

[3]*HOD AIIT, Amity University, Lucknow*

[1]tnvagrawal2909@gmail.com

[2]ambuj4u@gmail.com

[3]sksingh1@amity.edu

Abstract— **Cloud computing is a set of IT services that are provided to a customer over a network with the ability to scale up or down the service requirements. Cloud computing has been imagined as the next generation architecture for IT enterprises. In cloud data is transferred among the server and client. In this paper we have discussed about the various issues and challenges of cloud computing security.**

Keywords— ***Cloud computing, privacy, infrastructure, virtualization***

I. Introduction

Cloud computing has been presented as the next generation architecture for the IT enterprise. In the traditional approach the IT services under proper physical, logical and personnel controls. Cloud computing comprise of activities such as the use of social networking sites and interpersonal computing. Cloud computing is mainly concerned with accessing online software application, data storage and processing power. Several trends are opening up the era of Cloud Computing, which is an internet-based development and use of computer technology. The important force behind cloud computing is the presence of broadband and wireless networking, falling storage costs and progressive improvements in Internet computing software.

II. Related Works done

The major security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access-information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water, (2) regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location – depending on contracts, some clients might never know what country or what jurisdiction their data is located (4) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (5) recovery-every provider should have a disaster recovery protocol to protect user data (6) investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation (7) long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm.[2] The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers.[3] ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[4] Balachandra et al, 2009 discussed the security

SLA's specification and objectives related to data locations, segregation and data recovery.[5] Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.[6] Bernd et al, 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related.[7] Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model.[8] Ragovind et al, (2010) discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise.[9] Morsy et al, 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives.[10] A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.[11] Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

III. SECURITY ISSUES IN CLOUD COMPUTING

Cloud Deployment Models

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location. Four deployment models are usually distinguished, namely public, private, community and hybrid cloud service usage.

Public Cloud: The deployment of a public cloud computing system is characterized on the one hand by the public availability of the cloud service offering and on the other hand by the public network that is used to communicate with the cloud service. Public clouds are less secure than the other clouds because it produces an additional burden of ensuring all applications and data accessed on the public clouds are not subjected to malicious attacks.

Private Cloud: Private cloud computing systems emulate public cloud service offerings within an organization's boundaries to make services accessible for one designated organization. Private cloud computing systems make use of virtualization solutions and focus on consolidating distributed IT services often within data centers belonging to the company. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure.

Hybrid Cloud: A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models. For example, a cloud consumer may choose to deploy cloud services processing sensitive data to a private cloud and other, less sensitive cloud services to a public cloud. The result of this combination is a hybrid deployment model. Hybrid deployment model can be complex and challenging to create and maintain due to the potential disparity in cloud environment and the fact that management responsibilities are split between the public cloud provider and private cloud provider.

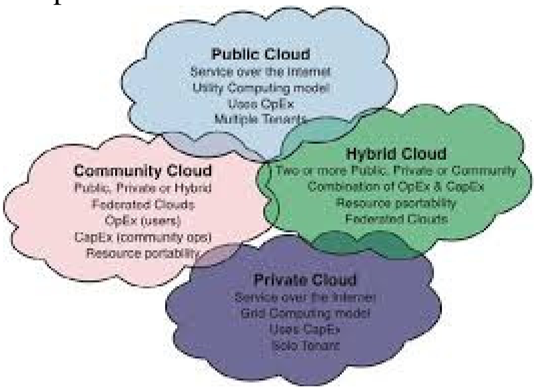

Fig. 1 Example of Cloud Deployment Models

Community Cloud: In a community cloud, organizations with similar requirements share a cloud infrastructure. It may be understood as a generalization of a private cloud, a private cloud being an infrastructure which is only accessible by one certain organization. Membership in the community does not necessarily guarantee access to or control of all the cloud's IT resources. Parties outside the community are generally not granted access unless allowed by the community.

Cloud Computing Service Delivery Models

Service delivery in Cloud computing comprise of three service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS).

Infrastructure-as-a-Service(IaaS): The services on the infrastructure layer are used to access essential IT resources that are combined under the heading Infrastructure-as-a-Service (IaaS). These essential IT resources include services linked to computing resources, data storage resources, and the communications channel. They enable existing applications to be provisioned on cloud resources and new services implemented on the higher layers. The cloud has a compelling value proposition in terms of cost, but 'out of box' IaaS only provides basic security(perimeter firewall, load balancing etc) and applications moving into the cloud will need higher levels of security provided at the host.

Platform-as-a-Service(PaaS): PaaS comprises the environment for developing and provisioning cloud applications. The principal users of this layer are developers seeking to develop and run a cloud application for a particular platform. They are supported by the platform operators with an open or proprietary language, a set of essential basic services to facilitate communication, monitoring, or service billing, and various other components, for instance to facilitate startup or ensure an application's scalability and/or elasticity. Clients using PaaS service transfer even more cost from capital investment to operational expenses but must acknowledge the additional constraints. The use of Virtual machines act as a catalyst in PaaS layer cloud computing. They must be protected against malicious attacks such as cloud malware.

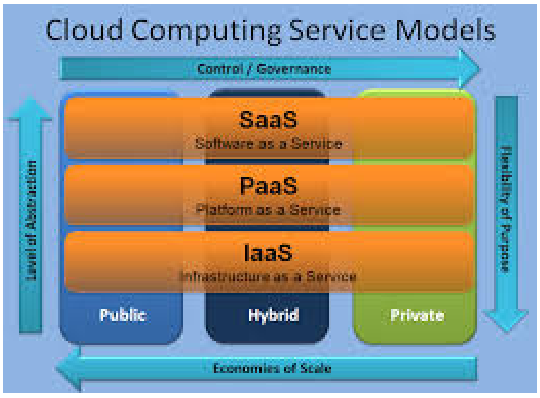

Fig. 1 Example of Cloud Computing Service Delivery Models

Software-as-a-Service (SaaS): Software-as-a-Service provides complete applications to a cloud's end user. It is mainly accessed through a web portal and service oriented architectures based on web service technologies. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important

IV. Challenges in Cloud Computing

Companies are increasingly aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. Like any new technology, the adoption of cloud computing is not free from issues. Some of the most important challenges are as follows:

A. Security and Privacy: The top most concern that everybody seem to agree as a challenge with cloud is security. The data security and privacy concerns ranks top on almost all of the surveys. The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data will reside outside the corporate firewall raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behavior across servers.

B. Service Delivery and Billing: It is difficult to assess the costs involved due to the on-demand nature of the services. Budgeting and assessment of the cost will be very difficult unless the provider has some good and comparable benchmarks to offer. The service-level agreements (SLAs) of the provider are not adequate to guarantee the availability and scalability. Businesses will be reluctant to switch to cloud without a strong service quality guarantee.

C. Service Quality: Service quality is one of the biggest factors that the enterprises consider as a reason for not moving their business applications to cloud. They feel that the SLAs provided by the cloud providers today are not sufficient to guarantee the requirements for running a production applications on cloud especially related to the availability, performance and scalability. In most cases, enterprises get refunded for the amount of time the service was down but most of the current SLAs down cover business loss. Without proper service quality guarantee enterprises are not going to host their business critical infrastructure in the cloud.

D. Costing model: Cloud consumers must consider the tradeoffs amongst computation, communication and integration. While migrating to the cloud can significantly reduce the infrastructure cost, it raise the cost of data communication i.e. the cost of transferring an organization's data to and from public and community cloud and cost per unit of computing resource is likely to be higher. This problem is very high if we use hybrid cloud.

E. Performance and Bandwidth Cost: Businesses can save money on hardware but they have to spend more for the bandwidth. This can b a low cost for smaller application but can be high for data-intensive application. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this, many businesses are waiting for a reduced cost before switching to the cloud.

F. Performance / Insufficient responsiveness over network: Delivery of complex services through the network is clearly impossible if the network bandwidth is not adequate. Many of the businesses are waiting for improved bandwidth and lower costs before they consider moving into the cloud. Many cloud applications are still too bandwidth intensive.

G. Integration: Many applications have complex integration needs to connect to other cloud applications as well as other on-premise applications. These include integrating existing cloud applications with existing enterprise applications and data structures. There is a need to connect the cloud application with the rest of the enterprise in a simple, quick and cost effective way.

H. Recoverability: Data stored in the cloud is subjected to regular integrity tests to guarantee its recoverability. Most cloud service providers replicate data three of four times instead of making real backups. This means they can recover from disk crashes and major disasters. However, most service providers do not guarantee the backup and recovery of data which is "accidentally" deleted by the end-users themselves. A government body must therefore make or arrange its own backups.

Another problem is that data in clouds can be stored indefinitely. Depending on the type of data and the applicable legislation, this may not be permitted. Service providers only process and store data. So, they may have insufficient knowledge of statutory retention periods or mandatory clearances. Public authorities have an important role to play in this regard. Cloud providers can guarantee that information has actually been destroyed, but the owner of the data needs to ensure that the destruction has been initiated.

I. Protection: Privacy measures protect personal information in such a way that others cannot access it. Various identity and access management systems support cloud services with a wide range of privacy and security measures. These include low security level with password-based authentication, to high security level with attribute-based authentication systems. The latter systems use state-of-the-art privacy-supporting certificates. Efficient process organization is also important in the event that the authorities raise any questions.

V. CONCLUSION

Cloud computing is an important trend in the field of information provision and related ICT. It turns computer processing power and data storage into a utility for collective use, as has long been the case of gas, water, and electricity. The rise of cloud computing has been particularly strong, is set to continue, and is irreversible. In view of the advantages for government organizations, cloud computing should also be trusted and supported within the public sector, both at central and local government levels and within executive agencies.

REFERENCES

[1] Kuyoro S. O., Ibikunle F. & Awodele O., “Cloud Computing Issues and Challenges,”

[2] J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” Infoworld

[3] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010

[4] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security.”

[5] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC

[6] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges."

[7] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing

[8] S. Subashini, and V. Kavitha. (2010) “A survey on security issues in service delivery models of cloud computing.” J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul.,2010.

[9] S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing.

[10] M. A. Morsy, J. Grundy and Müller I. “An Analysis of the Cloud Computing Security Problem” In PROC APSEC 2010

[11] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org[Mar.19,2010]